





RODO - aktualności

Data publikacji: 10.10.2025

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01

TSUE przyznaje 50 000 euro odszkodowania za naruszenie prywatności

02

NSA: organ nadzorczy prawidłowo nakazał usunięcie danych spółce windykacyjnej

03

Prezes UODO: Ofiarom deepfake'ów należy się lepsza ochrona

04

Wadowice zhackowane, dane mieszkańców mogły zostać wykradzione

05

NASK: 28% nastolatków w Polsce doświadczyło cyberataków

O naszej książce: poznaj **RODOLOGIĘ**

- ✔ Autorska koncepcja pięciu filarów
- ✔ Gotowe sprawdzone rozwiązania
- ✔ Automatyzacja rozwiązań
- ✔ Prosty język, przykłady i schematy
- ✔ Myślenie procesowe by default
- ✔ Ponad 500 stron w pięknej, premium formie



Razem z książką otrzymasz dostęp do aplikacji SODO z Modelowym RCP

01 TSUE przyznaje 50 000 euro odszkodowania za naruszenie prywatności

- Sprawa dotyczy greckiej naukownicy, która prowadziła projekt badawczy finansowany z funduszy UE. W toku późniejszej kontroli wykryto nieprawidłowości finansowe, a Europejski Urząd ds. Zwalczenia Nadużyć Finansowych (OLAF) opublikował komunikat, który umożliwił identyfikację badaczki, co doprowadziło do złożenia przez nią skargi za naruszenie ochrony danych osobowych i prawa do domniemania niewinności.
- Sprawa rozpoczęła się od projektu badawczego finansowanego z dotacji UE, zawartej w 2008 r. między Komisją Europejską a greckim uniwersytetem.
- Po kontroli finansowej, OLAF zakwestionował część wydatków jako niekwalifikowalne i zażądał ich zwrotu.
- W 2020 r. OLAF opublikował komunikat prasowy informujący o dochodzeniu, ujawniając informacje umożliwiające identyfikację badaczki.
- W wyniku tej publikacji badaczka wniosła pozew przeciw Komisji Europejskiej (odpowiedzialnej za OLAF), domagając się ponad 1 mln euro odszkodowania za naruszenie prywatności i dóbr osobistych.
- Początkowo, w 2022 r., Sąd UE oddalił pozew, uznając, że nie doszło do wystarczająco poważnego naruszenia prawa przez OLAF.
- Trybunał uchylił jednak ten wyrok w marcu 2024 r., przyznając rację skarżącej w zakresie naruszeń przepisów o ochronie danych osobowych i domniemaniu niewinności.
- W październiku 2025 r. Sąd UE przyznał naukownicy 50 000 euro odszkodowania.
- **Kluczowe argumenty sądu za przyznaniem odszkodowania:**
- OLAF przetworzył dane osobowe naukownicy w sposób niezgodny z prawem – ujawniono informacje takie jak wiek, płeć, obywatelstwo, pokrewieństwo z osobą kierującą laboratorium, co pozwalało na jej identyfikację.

Źródło: <https://judykatura.pl/tsue-przyznaje-50-000-euro-odszkodowania-za-naruszenie-prywatnosci/>

01 cd. TSUE przyznaje 50 000 euro odszkodowania za naruszenie prywatności

- Ujawnione dane nie były niezbędne do informowania opinii publicznej, przez co naruszono przepisy o ochronie danych osobowych.
- Doszło do istotnego naruszenia zasady domniemania niewinności oraz obowiązku neutralności i bezstronności w działaniu OLAF, wynikających z Karty Praw Podstawowych UE i aktów prawnych UE.
- **Wniosek:**
- Sąd UE uznał, że działania OLAF w przedmiotowej sprawie naruszyły istotne zasady prawa unijnego, w tym ochronę danych osobowych i domniemanie niewinności, co skutkowało obowiązkiem Komisji Europejskiej zapłaty odszkodowania w wysokości 50 000 euro poszkodowanej naukowczynie.

Źródło: <https://judykatura.pl/tsue-przyznaje-50-000-euro-odszkodowania-za-naruszenie-prywatnosci/>

02 NSA: organ nadzorczy prawidłowo nakazał usunięcie danych spółce windykacyjnej

- **Kontekst sprawy:** Naczelny Sąd Administracyjny (NSA) rozpoznał skargę kasacyjną spółki, która została złożona na wyrok Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie. Sprawa dotyczyła decyzji Prezesa Urzędu Ochrony Danych Osobowych (UODO) z lipca 2021 r., nakazującej usunięcie danych osobowych (imię, nazwisko, numer telefonu) byłego dłużnika.
- **Podstawa prawna sporu:** Spółka przetwarzała dane osobowe na podstawie art. 6 ust. 1 lit. f RODO – czyli w oparciu o uzasadniony interes prawny, jakim było dochodzenie roszczeń finansowych wobec byłego dłużnika D.B.
- **Stanowisko Prezesa UODO:** Prezes uznał, że po zakończeniu działań windykacyjnych w lipcu 2018 r. nie istniała już podstawa prawna do dalszego przetwarzania danych osobowych, bo pierwotny cel – dochodzenie roszczeń – został osiągnięty.
- **Argumenty Spółki:** Spółka twierdziła, że nadal może przetwarzać dane osobowe byłego dłużnika, ponieważ istnieje potencjalna potrzeba ich zachowania w celu obrony przed ewentualnymi przyszłymi roszczeniami.
- **Wyrok WSA:** WSA w Warszawie oddalił skargę spółki, uznając, że Prezes UODO nie naruszył przepisów krajowych ani unijnych i miał prawo wydać decyzję nakazującą usunięcie danych.
- **Rozstrzygnięcie NSA:** Naczelny Sąd Administracyjny oddalił skargę kasacyjną, uznając, że:
 - Spółka faktycznie przetwarzała dane jako administrator, a nie podmiot przetwarzający działający na podstawie umowy powierzenia.
 - Po zakończeniu działań windykacyjnych brak było podstaw do przetwarzania danych na podstawie art. 6 ust. 1 lit. f RODO.
 - Organ nadzorczy (UODO) miał prawo wydać decyzję nakazującą usunięcie danych osobowych, kierowaną do administratora danych.

Źródło: <https://judykatura.pl/nsa-organ-nadzorczy-prawidlowo-nakazal-usuniecie-danych-spolce-windykacyjnej/>

02 cd. NSA: organ nadzorczy prawidłowo nakazał usunięcie danych spółce windykacyjnej

- Wnioski końcowe:
 - Administrator danych musi wykazać obecność rzeczywistego i aktualnego interesu prawnego dla dalszego przetwarzania danych osobowych.
 - Gdy pierwotny cel przetwarzania danych ustaje (np. zakończona windykacja), dalsze przechowywanie danych wymaga nowej, jednoznacznie uzasadnionej podstawy prawnej.
 - NSA potwierdził uprawnienie Prezesa UODO do wydania decyzji o usunięciu danych również wobec administratora, nie tylko wobec podmiotu przetwarzającego.

Źródło: <https://judykatura.pl/nsa-organ-nadzorczy-prawidlowo-nakazal-usuniecie-danych-spolce-windykacyjnej/>

03 Prezes UODO: Ofiarom deepfake'ów należy się lepsza ochrona

- **Kontekst:** Deepfake to technologia oparta na sztucznej inteligencji, która pozwala tworzyć realistyczne, ale fałszywe obrazy, nagrania audio i wideo, przypominające prawdziwe osoby lub wydarzenia. Technologia ta może być wykorzystywana do dezinformacji, ośmieszania, szantażu czy kradzieży tożsamości.
- **Prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski, apeluje o pilną zmianę prawa** w związku z rosnącym zagrożeniem związanym z łatwym dostępem do narzędzi AI umożliwiających tworzenie deepfake'ów.
- **W obecnym stanie prawnym brakuje regulacji**, które wprost odnosiłyby się do rozpowszechniania deepfake'ów. Obowiązujące przepisy, takie jak ochrona dóbr osobistych, prawo autorskie, RODO czy kodeks karny, nie są wystarczające w kontekście nowych technologii.
- **Unijne rozporządzenie AI Act**, które zacznie obowiązywać od 2 sierpnia 2026 r., wprowadzi regulacje dotyczące deepfake'ów. Będą one jednak dotyczyć wyłącznie materiałów wygenerowanych lub zmanipulowanych przez sztuczną inteligencję.
- **Nie wszystkie fałszywe treści będą objęte unijną regulacją** – np. fotomontaże stworzone w tradycyjnych programach graficznych nie będą objęte przepisami AI Act, mimo że mogą naruszać dobra osobiste.
- **Deepfake różni się od fotomontażu** tym, że jego stworzenie dzięki AI jest znacznie prostsze i nie wymaga specjalistycznych umiejętności. Obecnie nawet dzieci mogą tworzyć bardzo realistyczne, fałszywe materiały.
- **Prezes UODO zwrócił się do Ministra Cyfryzacji** z wnioskiem o rozpoczęcie prac legislacyjnych nad przepisami krajowymi, które będą:
 - regulować odpowiedzialność za wykorzystywanie deepfake'ów do szkodliwych celów,

Źródło: <https://www.prawo.pl/biznes/deepfake-a-prawo-prezes-uodo-apeluje-o-nowe-regulacje,535237.html>

03

cd. Prezes UODO: Ofiarom deepfake'ów należy się lepsza ochrona

- zapewniać poszkodowanym skuteczną i szybką ochronę swoich danych oraz wizerunku.
- **Technologia deepfake niesie poważne ryzyko wykorzystania w przestępstwach** takich jak kradzież tożsamości, oszustwa czy działania naruszające prywatność.
- **Wzmocnienie ochrony prawnej ofiar deepfake'ów** jest konieczne, aby nadążyć za tempem rozwoju technologii bazujących na sztucznej inteligencji.

Źródło: <https://www.prawo.pl/biznes/deepfake-a-prawo-prezes-uodo-apeluje-o-nowe-regulacje.535237.html>

04 Wadowice zhackowane, dane mieszkańców mogły zostać wykradzione

- **Kontekst:** W niedzielę doszło do cyberataku typu ransomware na infrastrukturę IT Urzędu Miejskiego w Wadowicach. Atak zakłócił działanie systemów przechowujących dane mieszkańców.
- **Natura ataku:** Dane zostały zaszyfrowane, co wskazuje na działanie o charakterze przestępczym – możliwe, że mające na celu wymuszenie okupu.
- **Zagrożenie dla mieszkańców:** Istnieje wysokie ryzyko, że dane osobowe mieszkańców gminy Wadowice zostały nie tylko zaszyfrowane, ale również wykradzione. Mogą one zostać upublicznione w internecie – zwłaszcza w tzw. Darknecie.
- **Potencjalne konsekwencje:** Opublikowanie danych może doprowadzić do:
 - kradzieży tożsamości,
 - oszustw finansowych,
 - ataków socjotechnicznych (np. podszywanie się pod urzędników lub banki),
 - naruszenia prywatności – dostęp do informacji o nieruchomościach, podatkach czy treści składanych wniosków.
- **Rekomendacje dla mieszkańców Wadowic:**
 - Natychmiastowe zastrzeżenie numeru PESEL – w celu zapobieżenia wyłudzeniom finansowym i innym nadużyciom.
 - Ignorowanie i przerywanie wszelkich kontaktów telefonicznych oraz e-mailowych, w których ktoś będzie prosił o dodatkowe dane – nawet jeśli zna już część danych i podaje się za przedstawiciela urzędu, banku czy innej instytucji.

Źródło: <https://niebezpiecznik.pl/post/wadowice-zhackowane-dane-mieszkancow-mogly-zostac-wykradzione/>

04 cd. Wadowice zhackowane, dane mieszkańców mogły zostać wykradzione

- W przypadku wątpliwości – samodzielny kontakt z danym urzędem lub instytucją w sposób oficjalny i bez pośredników.
- **Brak informacji o sprawcach:** Na ten moment nie ujawniono, która grupa hakerska odpowiada za atak. Sposób działania sugeruje jednak standardowy schemat działania grup ransomware.
- **Wnioski:** Incydent pokazuje, jak ważne jest przygotowanie na zagrożenia cybernetyczne oraz szybka i odpowiednia reakcja zarówno na poziomie instytucji publicznych, jak i indywidualnych użytkowników.

Źródło: <https://niebezpiecznik.pl/post/wadowice-zhackowane-dane-mieszkancow-mogly-zostac-wykradzione/>

05 NASK: 28% nastolatków w Polsce doświadczyło cyberataków

- **Kontekst:** Raport dotyczy cyberzagrożeń i ochrony danych osobowych wśród młodzieży w Polsce. Zwraca uwagę na rosnące ryzyko ataków, niską świadomość zagrożeń oraz niewystarczającą ochronę prywatności nastolatków.
- **Cyberzagrożenia:**
 - 28% nastolatków doświadczyło cyberataku, głównie włamań na konta w mediach społecznościowych i e-mail.
 - 4% młodych osób doświadczyło kradzieży tożsamości lub podszywania się pod inną osobę.
 - Starsze dzieci są bardziej narażone na cyberzagrożenia ze względu na większą aktywność online.
- **Kontrola rodzicielska i ochrona prywatności:**
 - Tylko 13% nastolatków korzysta z filtrów blokujących niebezpieczne treści, mimo że 28% rodziców deklaruje ich stosowanie.
 - Najczęstsza forma kontroli to limity czasu spędzanego online (45%).
 - Rzadziej stosuje się monitoring aktywności dziecka (ok. 11–12%).
 - Wraz z wiekiem dzieci rośnie ich samodzielność i zmniejsza się poziom nadzoru.
- **Świadomość zagrożeń prywatności:**
 - Ponad 25% nastolatków doświadczyło przemocy w internecie z powodu tożsamości, przekonań lub cech osobistych.
 - Aż 72% nastolatków nie zna pojęcia „deepfake” i nie potrafi rozpoznać cyfrowych manipulacji.

Źródło: <https://www.nask.pl/nastolatki>

05 cd. NASK: 28% nastolatków w Polsce doświadczyło cyberataków

- Wnioski dotyczące ochrony danych:
 - Niska świadomość zagrożeń: młodzież rzadko stosuje narzędzia ochrony prywatności (np. filtry, uwierzytelnianie dwuskładnikowe).
 - Rodzice mają mylne przekonanie o poziomie kontroli nad aktywnością dzieci w sieci.
 - Realne ryzyko: włamania, kradzież danych osobowych i dostęp do nielegalnych treści.
 - Raport wskazuje na konieczność systemowej edukacji w zakresie bezpieczeństwa cyfrowego i świadomego zarządzania danymi.
- **Rekomendacje:** Szkoły, rodzice i instytucje publiczne powinny wdrażać systemowe działania: edukację cyfrową, stosowanie technicznych środków ochrony i rozwijanie kompetencji cyfrowych młodzieży.

Źródło: <https://www.nask.pl/nastolatki>

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,
w szczególności rozpowszechniany i kopiowany.*